

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 1 0 月 1 2 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 2 9 8 2 4 4

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 2 9 8 2 4 4

出 願 人
Applicant(s): 日 本 電 信 電 話 株 式 有 限 公 司

2 0 0 5 年 9 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office.

中 嶋



== . AVAILABLE . ==

【書類名】

付 訂 願

【整理番号】

NTTH166071

【提出日】

平成16年10月12日

【あて先】

特許庁長官殿

【国際特許分類】

H04L 12/66

H04L 12/56

【発明者】

【住所又は居所】

東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】

濱田 雅樹

【特許出願人】

【識別番号】

000004226

【氏名又は名称】

日本電信電話株式会社

【代理人】

【識別番号】

100089118

【弁理士】

【氏名又は名称】

酒井 宏明

【選任した代理人】

【識別番号】

100114306

【弁理士】

【氏名又は名称】

中辻 史郎

【手数料の表示】

【予納台帳番号】

036711

【納付金額】

16,000円

【提出物件の目録】

【物件名】

特許請求の範囲 1

【物件名】

明細書 1

【物件名】

図面 1

【物件名】

要約書 1

【包括委任状番号】

0310351

【請求項 1】

サービス不能攻撃の攻撃対象となる通信機器が接続された LAN に設けられ ISP 網を介して前記通信機器に送信されたパケットを監視する監視装置および前記 ISP 網に設けられ前記 LAN に向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、

前記監視装置は、

前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手段と、

前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手段と

を備え、

前記制限装置は、

前記防御要求情報に基づいて前記 ISP 網を介して前記通信機器に送信されるパケットを制限するパケット制限手段を備えたことを特徴とするサービス不能攻撃防御システム。

【請求項 2】

前記監視装置は、前記通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成手段をさらに備え、前記防御要求情報送信手段は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記制限装置の前記パケット制限手段は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項 1 に記載のサービス不能攻撃防御システム。

【請求項 3】

前記制限装置は、前記シグネチャを含む前記防御要求情報が適正なものであるか否かを判断するシグネチャ判断手段をさらに備え、前記パケット制限手段は、前記シグネチャ判断手段によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする請求項 2 に記載のサービス不能攻撃防御システム。

【請求項 4】

前記制限装置は、前記シグネチャに該当するパケットの特徴や量に関するレポートを生成するレポート生成手段と、前記レポートを前記監視装置に送信するレポート送信手段とをさらに備え、前記シグネチャ生成手段は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手段は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手段は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項 2 または 3 に記載のサービス不能攻撃防御システム。

【請求項 5】

前記制限装置は、前記防御要求情報を前記 ISP 網に設けられた他の前記制限装置に転送する転送手段をさらに備え、前記転送手段は、前記レポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば前記防御要求情報を他の前記制限装置に転送することを特徴とする請求項 4 に記載のサービス不能攻撃防御システム。

【請求項 6】

前記制限装置は、前記シグネチャ判断手段の判断結果を前記監視装置に送信する判断結果送信手段をさらに備え、前記監視装置の前記シグネチャ生成手段は、前記判断結果が前記シグネチャは適正でないことを表す場合に、該判断結果に基づいて前記通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することを特徴とする請求項 3 ～ 5 のいずれか一つに記載のサービス不能攻撃防御システム。

【請求項 7】

サービス不能攻撃の攻撃対象となる通信機器が接続された LAN に設けられ ISP 網を介して前記通信機器に送信されたパケットを監視する監視装置および前記 ISP 網に設けられ前記 LAN に向かうパケットを制限する制限装置で前記通信機器に対するサービス不

能攻撃を防御するサービス不能攻撃防御方法のついで、

前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知工程と、

前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信工程と

前記防御要求情報に基づいて前記 I S P 網を介して前記通信機器に送信されるパケットを制限するパケット制限工程と

を含んだことを特徴とするサービス不能攻撃防御方法。

【請求項 8】

前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成工程をさらに含み、前記防御要求情報送信工程は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項 7 に記載のサービス不能攻撃防御方法。

【請求項 9】

前記シグネチャを含む前記防御要求情報が適正なものであるか否かを前記制限装置が判断するシグネチャ判断工程をさらに含み、前記パケット制限工程は、前記シグネチャ判断工程によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする請求項 8 に記載のサービス不能攻撃防御方法。

【請求項 10】

前記シグネチャに該当するパケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成工程と、前記レポートを前記監視装置に送信するレポート送信工程とをさらに含み、前記シグネチャ生成工程は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信工程は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項 8 または 9 に記載のサービス不能攻撃防御方法。

【請求項 11】

サービス不能攻撃の攻撃対象となる通信機器が接続された L A N に設けられ I S P 網を介して前記通信機器に送信されたパケットを監視する監視装置および前記 I S P 網に設けられ前記 L A N に向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、

前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手順と、

前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手順と

前記防御要求情報に基づいて前記 I S P 網を介して前記通信機器に送信されるパケットを制限するパケット制限手順と

をコンピュータに実行させることを特徴とするサービス不能攻撃防御プログラム。

【請求項 12】

前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成手順をさらに含み、前記防御要求情報送信手順は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手順は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項 11 に記載のサービス不能攻撃防御プログラム。

【請求項 13】

前記シグネチャを含む前記防御要求情報が適正なものであるか否かを前記制限装置が判断するシグネチャ判断手順をさらに含み、前記パケット制限手順は、前記シグネチャ判断手順によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケット

を制限し、適正でないことを判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする請求項 1 2 に記載のサービス不能攻撃防御プログラム。

【請求項 1 4】

前記シグネチャに該当するパケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成手順と、前記レポートを前記監視装置に送信するレポート送信手順とをさらに含み、前記シグネチャ生成手順は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手順は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手順は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする請求項 1 2 または 1 3 に記載のサービス不能攻撃防御プログラム。

【発明の名称】 サービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラム

【技術分野】

【0001】

この発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたLANに設けられISP網を介して通信機器に送信されたパケットを監視する監視装置およびISP網に設けられかかるLANに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関し、特に、通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関する。

【背景技術】

【0002】

従来、ネットワークを介した攻撃としてサービス不能攻撃(分散型サービス不能攻撃を含む)が知られている。かかるサービス不能攻撃から通信機器を防御するサービス不能攻撃防御システムでは、攻撃対象となるサーバマシン(以下「通信機器」と言う)を、ISP(Internet Service Provider) 網に設けられたエッジルータが防御することになる。具体的には、サービス不能攻撃の1つであるSYN Flood攻撃から保護するため、攻撃対象となる通信機器を含むLAN(Local Area Network)と接続されているISP網のエッジルータは、LANの出口回線にて、かかる通信機器を送信先とするSYNパケットのトラフィック量に対して閾値を設け、この閾値を超えた部分のSYNパケットを廃棄していた(例えば、特許文献1参照)。

【0003】

【特許文献1】 特開2004-166029号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、従来のサービス不能攻撃防御システムにおいては、ISP側で通信機器に送信されるパケットの内容を監視・判断し制御する必要があるが、攻撃かどうかは情報の解釈が必要であり受け取り手でないと判断できない場合が多いため、通信の秘密順守や本来業務の範囲を逸脱しないようにする必要性から、攻撃が予め自明な一部のケースを除きISP側で実施するには限界があるといった課題があった。

【0005】

本発明は、上述した従来技術による問題点を解消するためになされたものであり、ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムを提供することを目的とする。

【課題を解決するための手段】

【0006】

上述した課題を解決し、目的を達成するため、本発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたLANに設けられISP網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ISP網に設けられ前記LANに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、前記監視装置は、前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知手段と、前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手段とを備え、前記制限装置は、前記防御要求情報に基づいて前記ISP網を介して前記通信機器に送信されるパケットを制限するパケット制限手段を備えたことを特徴とする。

この発明によれば、監視装置が通信機器に対するパケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてISP網を介して前記通信機器に送信されるパケットを制限することとしたので、ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【 0 0 0 8 】

また、本発明は、上記発明において、前記監視装置は、前記通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成手段をさらに備え、前記防御要求情報送信手段は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記制限装置の前記パケット制限手段は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【 0 0 0 9 】

この発明によれば、監視装置が通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのパケットを制限することとしたので、攻撃を行うパケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるパケットを制限することができ、もってISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【 0 0 1 0 】

また、本発明は、上記発明において、前記制限装置は、前記シグネチャを含む前記防御要求情報が適正なものであるか否かを判断するシグネチャ判断手段をさらに備え、前記パケット制限手段は、前記シグネチャ判断手段によって適正であると判断されたシグネチャに該当する前記通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのパケットを制限しないことを特徴とする。

【 0 0 1 1 】

この発明によれば、制限装置がシグネチャを含む防御要求情報が適正なものであるか否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのパケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのパケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、パケットの制限が行われないため、他のLANに送信されるパケット等のような監視装置側で制限を要求してはならないパケットが制限装置によって制限されることを防止することができる。

【 0 0 1 2 】

また、本発明は、上記発明において、前記制限装置は、前記シグネチャに該当するパケットの特徴や量に関するレポートを生成するレポート生成手段と、前記レポートを前記監視装置に送信するレポート送信手段とをさらに備え、前記シグネチャ生成手段は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手段は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限手段は、前記新たなシグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【 0 0 1 3 】

この発明によれば、制限装置がシグネチャに該当するパケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのパケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるパケットを制限し、その後にレポートに基づいて攻撃するパケットを特定して通信機器に対する攻撃を行わないパケットの制限を解除することができる。

【 0 0 1 4 】

また、本発明は、上記発明において、前記制限装置は、前記防御要求情報を前記ISP

報に設けられた他の前記制限装置に転送する転送手段をさらに備え、前記転送手段は、前記レポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば前記防御要求情報を他の前記制限装置に転送することを特徴とする。

【0015】

この発明によれば、制限装置がレポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば防御要求情報を他の制限装置に転送することとしたので、監視装置がかかるレポートに基づいて本来制限すべきでないパケットの通過制限解除を制限装置に依頼することにより、制限装置が行う通過制限をより適正化することができる。

【0016】

また、本発明は、上記発明において、前記制限装置は、前記シグネチャ判断手段の判断結果を前記監視装置に送信する判断結果送信手段をさらに備え、前記監視装置の前記シグネチャ生成手段は、前記判断結果が前記シグネチャは適正でないことを表す場合に、該判断結果に基づいて前記通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することを特徴とする。

【0017】

この発明によれば、制限装置がシグネチャ判断の判断結果を監視装置に送信し、監視装置は、受け取った判断結果がシグネチャは適正でないことを表す場合に、この判断結果に基づいて通信機器に対する攻撃を行うパケットの特徴を表す新たなシグネチャを生成することとしたので、制限装置が不適正な通過制限を実行することを防止することができる。

【0018】

また、本発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたLANに設けられISP網を介して前記通信機器に送信されたパケットを監視する監視装置および前記ISP網に設けられ前記LANに向かうパケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記監視装置が前記通信機器に対する前記パケットによる攻撃を検知する攻撃検知工程と、前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信工程と前記防御要求情報に基づいて前記ISP網を介して前記通信機器に送信されるパケットを制限するパケット制限工程とを含んだことを特徴とする。

【0019】

この発明によれば、監視装置が通信機器に対するパケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてISP網を介して前記通信機器に送信されるパケットを制限することとしたので、ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【0020】

また、本発明は、上記発明において、前記通信機器に対する攻撃をおこなうパケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成工程をさらに含み、前記防御要求情報送信工程は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記パケット制限工程は、前記シグネチャに該当する前記通信機器向けのパケットを制限することを特徴とする。

【0021】

この発明によれば、監視装置が通信機器に対する攻撃を行うパケットの特徴を表すシグネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのパケットを制限することとしたので、攻撃を行うパケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるパケットを制限することができ、もってISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【0022】

また、本発明は、上記発明において、前記シグネチャを含む前記防御要求情報が適正な

ものであるが、前記制限装置が判断するシグネチャ判断工程によって適正であると判断されたシグネチャに該当する前記通信機器向けのバケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのバケットを制限しないことを特徴とする。

【0023】

この発明によれば、制限装置がシグネチャを含む防御要求情報が適正なものであるか否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのバケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのバケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、バケットの制限が行われないため、他のLANに送信されるバケット等のような監視装置側で制限を要求してはならないバケットが制限装置によって制限されることを防止することができる。

【0024】

また、本発明は、上記発明において、前記シグネチャに該当するバケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成工程と、前記レポートを前記監視装置に送信するレポート送信工程とをさらに含み、前記シグネチャ生成工程は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信工程は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記バケット制限工程は、前記新たなシグネチャに該当する前記通信機器向けのバケットを制限することを特徴とする。

【0025】

この発明によれば、制限装置がシグネチャに該当するバケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのバケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるバケットを制限し、その後にレポートに基づいて攻撃するバケットを特定して通信機器に対する攻撃を行わないバケットの制限を解除することができる。

【0026】

また、本発明は、サービス不能攻撃の攻撃対象となる通信機器が接続されたLANに設けられISP網を介して前記通信機器に送信されたバケットを監視する監視装置および前記ISP網に設けられ前記LANに向かうバケットを制限する制限装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、前記監視装置が前記通信機器に対する前記バケットによる攻撃を検知する攻撃検知手順と、前記攻撃に対する防御の要求を表す防御要求情報を前記制限装置に送信する防御要求情報送信手順と前記防御要求情報に基づいて前記ISP網を介して前記通信機器に送信されるバケットを制限するバケット制限手順とをコンピュータに実行させることを特徴とする。

【0027】

この発明によれば、監視装置が通信機器に対するバケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてISP網を介して前記通信機器に送信されるバケットを制限することとしたので、ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【0028】

また、本発明は、上記発明において、前記通信機器に対する攻撃をおこなうバケットの特徴を表すシグネチャを前記監視装置が生成するシグネチャ生成手順をさらに含み、前記防御要求情報送信手順は、前記シグネチャを含む前記防御要求情報を前記制限装置に送信し、前記バケット制限手順は、前記シグネチャに該当する前記通信機器向けのバケットを制限することを特徴とする。

【0029】

この発明によれば、監視装置が通信機器に対する攻撃を行うバケットの特徴を表すシグ

ハッシュを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのバケットを制限することとしたので、攻撃を行うバケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるバケットを制限することができ、もってISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【0030】

また、本発明は、上記発明において、前記シグネチャを含む前記防御要求情報が適正なものであるか否かを前記制限装置が判断するシグネチャ判断手順をさらに含み、前記バケット制限手順は、前記シグネチャ判断手順によって適正であると判断されたシグネチャに該当する前記通信機器向けのバケットを制限し、適正でないと判断されたシグネチャに該当する前記通信機器向けのバケットを制限しないことを特徴とする。

【0031】

この発明によれば、制限装置がシグネチャを含む防御要求情報が適正なものであるか否かを判断し、適正であると判断されたシグネチャに該当する通信機器向けのバケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのバケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、バケットの制限が行われないため、他のLANに送信されるバケット等のような監視装置側で制限を要求してはならないバケットが制限装置によって制限されることを防止することができる。

【0032】

また、本発明は、上記発明において、前記シグネチャに該当するバケットの特徴や量に関するレポートを前記制限装置が生成するレポート生成手順と、前記レポートを前記監視装置に送信するレポート送信手順とをさらに含み、前記シグネチャ生成手順は、前記レポートに基づいて新たなシグネチャを生成し、前記防御要求情報送信手順は、前記新たなシグネチャを含む前記防御要求情報を前記制限装置に送信し、前記バケット制限手順は、前記新たなシグネチャに該当する前記通信機器向けのバケットを制限することを特徴とする。

【0033】

この発明によれば、制限装置がシグネチャに該当するバケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのバケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるバケットを制限し、その後にレポートに基づいて攻撃するバケットを特定して通信機器に対する攻撃を行わないバケットの制限を解除することができる。

【発明の効果】

【0034】

本発明によれば、監視装置が通信機器に対するバケットによる攻撃を検知して攻撃に対する防御の要求を表す防御要求情報を制限装置に送信し、制限装置は、監視装置から受け取った防御要求情報に基づいてISP網を介して前記通信機器に送信されるバケットを制限することとしたので、ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【0035】

また、本発明によれば、監視装置が通信機器に対する攻撃を行うバケットの特徴を表すシグネチャを生成し、生成したシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、受け取ったシグネチャに該当する通信機器向けのバケットを制限することとしたので、攻撃を行うバケットの特徴を表すシグネチャに基づいて制限装置で通信機器に送信されるバケットを制限することができ、もってISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができる。

【0036】

また、本発明によれば、制限装置がシグネチャを含む防護要求情報が適正なものである

が、口がを判断し、適正であると判断されたシグネチャに該当する通信機器向けのバケットを制限し、適正でないと判断されたシグネチャに該当する通信機器向けのバケットを制限しないこととしたので、シグネチャが適正なものでなかった場合には、バケットの制限が行われなため、他のLANに送信されるバケット等のような監視装置側で制限を要求してはならないバケットが制限装置によって制限されることを防止することができる。

【0037】

また、本発明によれば、制限装置がシグネチャに該当するバケットの特徴や量に関するレポートを生成し、生成したレポートを監視装置に送信し、監視装置は、受け取ったレポートに基づいて新たなシグネチャを生成して新たなシグネチャを含む防御要求情報を制限装置に送信し、制限装置は、新たなシグネチャに該当する通信機器向けのバケットを制限することとしたので、通信機器に対する攻撃があった場合に攻撃の容疑がかかるバケットを制限し、その後にレポートに基づいて攻撃するバケットを特定して通信機器に対する攻撃を行わないバケットの制限を解除することができる。

【0038】

また、本発明によれば、制限装置がレポート生成工程により生成されたレポートに基づいて転送の可否を判断し、転送が必要と判断したならば防御要求情報を他の制限装置に転送することとしたので、監視装置にかかるレポートに基づいて本来制限すべきでないバケットの通過制限解除を制限装置に依頼することにより、制限装置が行う通過制限をより適正化することができる。

【0039】

また、本発明によれば、制限装置がシグネチャ判断の判断結果を監視装置に送信し、監視装置は、受け取った判断結果がシグネチャは適正でないことを表す場合に、この判断結果に基づいて通信機器に対する攻撃を行うバケットの特徴を表す新たなシグネチャを生成することとしたので、制限装置が不適正な通過制限を実行することを防止することができる。

【発明を実施するための最良の形態】

【0040】

以下に添付図面を参照して、この発明に係るサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムの好適な実施の形態を詳細に説明する。

【実施例】

【0041】

図1は、本実施例に係るサービス不能攻撃防御システム1の構成を示すブロック図である。同図に示すサービス不能攻撃防御システム1は、通信機器3へのサービス不能攻撃を監視装置5および制限装置6で防御するシステムである。具体的には、LAN2上の監視装置5が通信機器3へのサービス不能攻撃を検知したならば（図1のステップ1）、攻撃の特徴を表すシグネチャを生成してかかるシグネチャを含む防御要求情報をISP網4上の制限装置6に送信する（図1のステップ2）。そして、防御要求情報を受信した制限装置6は、防御要求情報に含まれるシグネチャに基づいてサービス不能攻撃を行うバケットの通過を制限することにより防御を実行する（図1のステップ3）こととしている。

【0042】

従来、ISP網4上の制限装置6では、攻撃と思われるバケットが通過した場合であっても、攻撃かどうかはバケットに含まれる情報の解釈が必要であり受け取り手でないと判断できない場合が多いため、ISP網4を運営するISPは、通信の秘密順守や本来業務の範囲を逸脱しないようにする必要性から、攻撃が予め自明な一部のケースを除き、かかるバケットの制限を行うことができないという問題があった。本実施例では、バケットに含まれる情報の解釈をLAN2上の監視装置5が行い、監視装置5が検出した攻撃バケットの通過制限をISP網4上の制限装置6が行うこととしている。このため、本実施例によれば、ISPが通信の秘密を順守すると共に本来業務の範囲内で通信装置3を攻撃するバケットを効果的に制限することができる。

また、かかる制限装置 6 は、監視装置 5 が検出した攻撃パケットの通過制限を行った場合に、この通過制限の内容を表すレポートを監視装置 5 に送信することとしている。このため、監視装置 5 がかかるレポートに基づいて本来制限すべきでないパケットの通過制限解除を制限装置 6 に依頼することにより、制限装置 6 が行う通過制限をより適正化することができる。

【 0 0 4 4 】

さらに、かかる制限装置 6 は、監視装置 5 からパケットの通過制限を依頼された場合に、依頼内容が適正であるものについてのみ通過制限を実行することとしている。このため、制限装置 6 が不適正な通過制限を実行することを防止することができる。

【 0 0 4 5 】

次に、このサービス不能攻撃防御システム 1 のシステム構成について説明する。図 1 に示すように、このサービス不能攻撃防御システム 1 は、中小企業内に設けられた LAN 2 に設けられ、LAN 2 に接続された少なくとも 1 つの通信機器 3 に基幹回線網等の ISP 網 4 を介して送信されたパケットを監視する監視装置 5 と、LAN 2 を ISP 網 4 に接続する制限装置 6 とを備えている。なお、図 1 に示したサービス不能攻撃防御システム 1 の構成は一例を示すものであり、本発明のサービス不能攻撃防御システムは、複数の制限装置 6 を備えてもよく、各制限装置 6 に対して複数の監視装置 5 をそれぞれ備えてもよい。

【 0 0 4 6 】

監視装置 5 は、LAN 2 を構成するルータによって構成されている。なお、監視装置 5 は、LAN 2 に設けられたファイアウォール等によって構成してもよい。

【 0 0 4 7 】

図 2 は、図 1 に示した監視装置 5 の構成を示すブロック図である。監視装置 5 は、通信機器 3 に送信されるパケットによる攻撃を検知する攻撃検知部 10 と、攻撃に対する防御の要求を表す防御要求情報を制限装置 6 に送信する防御要求情報送信部 11 と、通信機器 3 に対する攻撃を行うパケットの特徴を表すシグネチャを生成するシグネチャ生成部 12 と、制限装置 6 および LAN 2 に設けられた各装置とそれぞれ通信を行うための通信インタフェース 13、14 と、パケットをルーティングするためのスイッチ 15 とを備えている。

【 0 0 4 8 】

攻撃検知部 10 は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図 3 は、攻撃検知条件の一例を示す図である。図 3 において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる 3 組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。

【 0 0 4 9 】

例えば、1 番目の検知条件は、宛先のアドレス情報が 192.168.1.1 であり (Dst=192.168.1.1/32)、トランスポート層のプロトコルが TCP (Transmission Control Protocol) であり (Protocol=TCP)、TCP ポート番号が 80 である (Port=80) パケットが検知対象となり、この検知対象のパケットの伝送レートが 500 kbps を超えた状態が 10 秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【 0 0 5 0 】

同様に、2 番目の検知条件は、宛先のアドレス情報が 192.168.1.2 であり (Dst=192.168.1.2/32)、トランスポート層のプロトコルが UDP (User datagram protocol) である (Protocol=UDP) パケットが検知対象となり、この検知対象のパケットの伝送レートが 300 kbps を超えた状態が 10 秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【 0 0 5 1 】

また、3 番目の検知条件は、宛先のアドレス情報が 192.168.1.0~192.168.1.255 の範囲

のである（例えば、192.168.1.0/24）のパケットが検知対象となり、この検知対象のパケットの伝送レートが1Mbpsを超えた状態が20秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0052】

このように、検知対象のパケットによる攻撃が攻撃検知部10によって検知されると、シグネチャ生成部12は、検知対象のパケットの特徴を表すシグネチャを生成するようになっている。例えば、図3における攻撃検知条件の1番目の検知条件に合う攻撃が検知された場合には、シグネチャ生成部12は、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であるパケットを示すシグネチャを生成する。なお、シグネチャは、対象となるパケットに対する制御方法としてシェーピングやフィルタリング等の処理の指定や、この処理に関するパラメータ等を含むようにしてもよい。

【0053】

防御要求情報送信部11は、シグネチャ生成部12によって生成されたシグネチャを含み、攻撃に対する防御の要求を表す防御要求情報を制限装置6に送信する処理部である。なお、防御要求情報送信部11は、パケットが送受信される伝送路7とは異なる通信経路で防御要求情報を送信するようにしてもよい。

【0054】

図1に示した制限装置6は、LAN2をISP網4に接続するエッジルータによって構成されている。なお、ここでは説明の便宜上制限装置6の構成を説明するが、他の制限装置8～9についても制限装置6と同様に構成されている。

【0055】

図4は、図1に示した制限装置6の構成を示すブロック図である。この制限装置6は、防御要求情報に基づいてISP網4を介して通信機器3に送信されるパケットを制限するパケット制限部20と、防御要求情報を他のパケット制限装置に転送する防御要求情報転送部21と、シグネチャを含む防護要求情報が適正なものであるか否かを判断するシグネチャ判断部22と、シグネチャ判断部22による判断結果を監視装置5に送信する判断結果送信部23と、シグネチャに当てはまるパケットの特徴や量に関するレポートを生成するレポート生成部24と、レポートを監視装置5に送信するレポート送信部25と、監視装置5およびISP網4に設けられた各装置とそれぞれ通信を行うための通信インタフェース26、27と、パケットをルーティングするためのスイッチ28とを備えている。

【0056】

シグネチャ判断部22は、監視装置5から送信された防御要求情報に含まれるシグネチャを含む防護要求情報が適正なものであるか否かを判断する処理部である。ここで、シグネチャ判断部22は、他のLANに送信されるパケット等のような監視装置5側で制限を要求してはならないパケットが制限装置6によって制限されることを防止する。

【0057】

パケット制限部20は、シグネチャ判断部22によってシグネチャを含む防護要求情報が適正なものであると判断された場合には、監視装置5から送信された防御要求情報に含まれるシグネチャに該当するパケットを制限する処理部である。

【0058】

シグネチャ判断部22による判断結果は、判断結果送信部23によって監視装置5に送信される。なお、判断結果送信部23は、パケットが送受信される伝送路7とは異なる通信経路で判断結果を送信するようにしてもよい。

【0059】

ここで、監視装置5のシグネチャ生成部12は、送信された判断結果に応じてシグネチャを再生成するようにしてもよい。例えば、防御要求情報送信部11によって送信された防御要求情報が、あるネットワークアドレスから送信されたパケットの制限を要求し、この要求が適正なものではないとシグネチャ判断部22によって判断された判断結果が判断結果送信部23によって送信された場合には、シグネチャ生成部12は、攻撃検知部10

をかし、サブプロットノリを判定し、上述したサブプロットノリが小サブプロットノリ内でトラフィックが高いホストから送信されたパケットを制限するようシグネチャを再生成する。

【0060】

なお、シグネチャ生成部12によるシグネチャの再生成は、判断結果送信部23によって送信された判断結果を見たLAN2の管理者によるオペレーションによって行われるようにしてもよい。

【0061】

レポート生成部24は、監視装置5から送信された防御要求情報に含まれるシグネチャに該当するパケットの特徴や量に関するレポートを生成する処理部である。例えば、レポート生成部24は、シグネチャに該当するパケットのヘッダ部に含まれる送信元のアドレス情報と、当該パケットの伝送量とを対応させるテーブルを含むレポートを生成する。

【0062】

レポート生成部24によって生成されたレポートは、レポート送信部25によって監視装置5に送信される。なお、レポート送信部25は、パケットが送受信される伝送路7とは異なる通信経路でレポートを送信するようにしてもよい。

【0063】

ここで、監視装置5のシグネチャ生成部12は、送信されたレポートに応じてシグネチャを再生成する。なお、このシグネチャ生成部12によるシグネチャの再生成は、レポート送信部25によって送信されたレポートを見たLAN2の管理者によるオペレーションによって行われるようにしてもよい。

【0064】

監視装置5の防御要求情報送信部11は、シグネチャ生成部12によって再生成されたシグネチャを含む防御要求情報を制限装置6に再送信し、制限装置6のパケット制限部20は、シグネチャ判断部22によってシグネチャを含む防護要求情報が適正なものであると判断された場合には、監視装置5から再送信された防御要求情報に含まれるシグネチャに該当するパケットを制限する。

【0065】

このように、かかるレポートに基づいてシグネチャを再生成することによって、通信機器3に対する攻撃を行っていないパケットや、通信機器3に対する攻撃を現に行っているパケット等を特定し、制限対象となるパケットを絞りこんだ制限を課していくことができる。したがって、通信機器3に対する攻撃を行っておらず本来制限すべきでないパケットの制限を解除することができる。

【0066】

防御要求情報転送部21は、監視装置5から送信された防御要求情報を制限装置6と同様に構成された他のパケット制限装置（例えば、図1に示したパケット制限装置8、9）に転送するか否かをレポート生成部24によって生成されたレポートに基づいて判断し、防御要求情報を他のパケット制限装置に転送すると判断した場合には、防御要求情報を他のパケット制限装置に転送する。

【0067】

以上のように構成されたサービス不能攻撃防御システム1について、図5～図7を用いてその動作を説明する。図5は、図2に示した監視装置5の攻撃検知動作を示すフローチャートである。

【0068】

まず、通信機器3に送信されるパケットによる攻撃が攻撃検知部10によって攻撃検知条件に基づいて検知されると（ステップS1）、攻撃が検知されたパケットの特徴を表すシグネチャがシグネチャ生成部12によって生成され（ステップS2）、生成されたシグネチャを含む防御要求情報が防御要求情報送信部11によって制限装置6に送信される（ステップS3）。

【0069】

ここで、防御要求情報の送信に際して制限装置6から送信されたシグネチャを含む防御要求情報が適正なものであるか否かの判断結果が通信インタフェース13に受信され（ステップS4）、この判断結果にシグネチャが適正なものではないことが示されている場合（ステップS5）には、この判断結果に基づいてシグネチャ生成部12によってシグネチャが再生成され（ステップS2）、再生成されたシグネチャを含む防御要求情報が防御要求情報送信部11によって制限装置6に再送信される（ステップS3）。

【0070】

また、制限装置6によって送信されたレポートが通信インタフェース13に受信された場合（ステップS6）には、受信されたレポートに基づいてシグネチャを再生成するか否かがシグネチャ生成部12によって判断され（ステップS7）、シグネチャを再生成すると判断された場合には、レポートに基づいてシグネチャ生成部12によってシグネチャが再生成され（ステップS2）、再生成されたシグネチャを含む防御要求情報が防御要求情報送信部11によって制限装置6に再送信される（ステップS3）。

【0071】

図6は、図4に示した制限装置6の防御要求情報受信動作を示すフローチャートである。監視装置5から送信された防御要求情報が通信インタフェース26に受信されると（ステップS10）、受信された防御要求情報に含まれるシグネチャおよびその他の情報が適正なものであるか否かがシグネチャ判断部22によって判断される（ステップS11）。

【0072】

防御要求情報に含まれるシグネチャおよびその他の情報が適正なものであるとシグネチャ判断部22によって判断された場合には、シグネチャがバケット制限部20に設定される（ステップS12）。また、防御要求情報に含まれるシグネチャおよびその他の情報が適正なものであるか否かのシグネチャ判断部22による判断の結果は、判断結果送信部23によって監視装置5に送信される（ステップS13）。

【0073】

図7は、図4に示した制限装置6のレポート送信動作を示すフローチャートである。バケット制限部20にシグネチャが設定されている場合（ステップS20）には、監視装置5から送信された防御要求情報に含まれるシグネチャに該当するバケットの特徴や量に関するレポートがレポート生成部24によって生成され（ステップS21）、生成されたレポートがレポート送信部25によって監視装置5に送信される（ステップS22）。

【0074】

また、レポート生成部24によって生成されたレポートに基づいて、通信インタフェース26に受信された防御要求情報をバケット制限装置8、9等の他のバケット制限装置に転送するか否かが防御要求情報転送部21によって判断され（ステップS23）、防御要求情報を他のバケット制限装置に転送すると判断された場合には、防御要求情報が防御要求情報転送部21によって他のバケット制限装置に転送される（ステップS24）。

【0075】

このように、レポート送信部25によって送信されたレポートに基づいて攻撃の終了が監視装置5で検知され、防御要求情報送信部11によって所定の防御要求情報が制限装置6に送信されることによってバケット制限部20によるバケットの制限が解除される。

【0076】

上述してきたように、サービス不能攻撃防御システム1によれば、LAN2側で通信機器3に対する攻撃が検知され、検知された攻撃の防御要求に基づいてISP網4側の制限装置6で通信機器3に送信されるバケットが制限されるため、ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器3を防御することができる。

【0077】

なお、上記実施例に示した監視装置および制限装置は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、監視装置のコンピュータのROM（Read Only Memory）等に通信機器を攻撃するバケットを検知するルーチン、制限装置

に対して防護要求情報を返信するルーチンを含むプログラムを記憶し、また、制限装置のコンピュータのROM等に通信機器へ攻撃を行うパケットの通過を防護要求情報に基づいて制限するルーチンを含むプログラムを記憶しておき、各装置がこれらのプログラムをCPUにロードして実行することにより、本発明に係る監視装置および制限装置を形成することができる。

【産業上の利用可能性】

【0078】

以上のように、本発明にかかるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムは、サービス不能攻撃から通信機器を防御する場合に適している。

【図面の簡単な説明】

【0079】

【図1】 本実施例に係るサービス不能攻撃防御システムの構成を示すブロック図である。

【図2】 図1に示した監視装置の構成を示すブロック図である。

【図3】 本実施例に係る攻撃検知条件の一例を示す図である。

【図4】 図1に示した制限装置の構成を示すブロック図である。

【図5】 図2に示した監視装置の攻撃検知動作を示すフローチャートである。

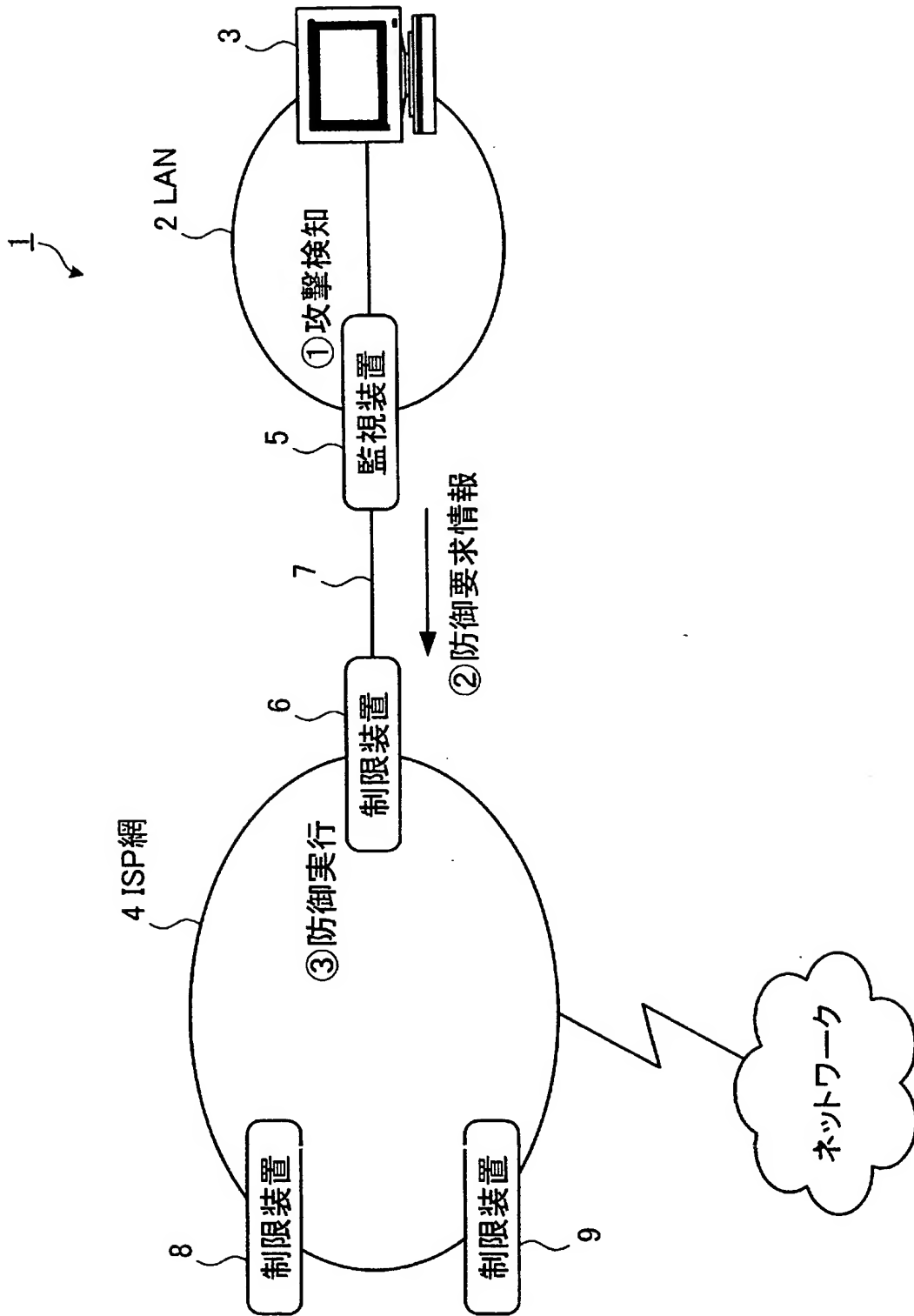
【図6】 図4に示した制限装置の防護要求情報受信動作を示すフローチャートである。

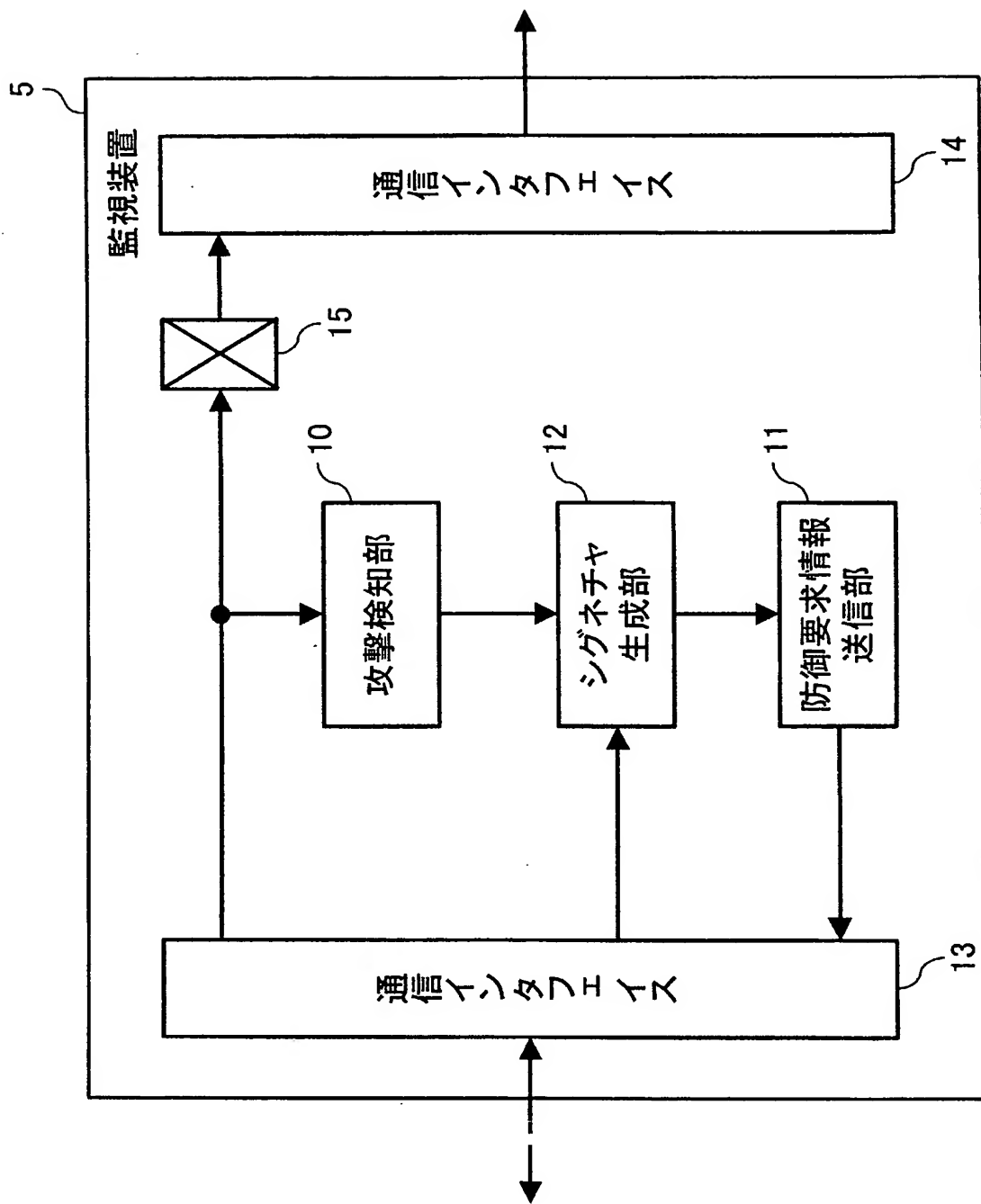
【図7】 図4に示した制限装置のレポート送信動作を示すフローチャートである。

【符号の説明】

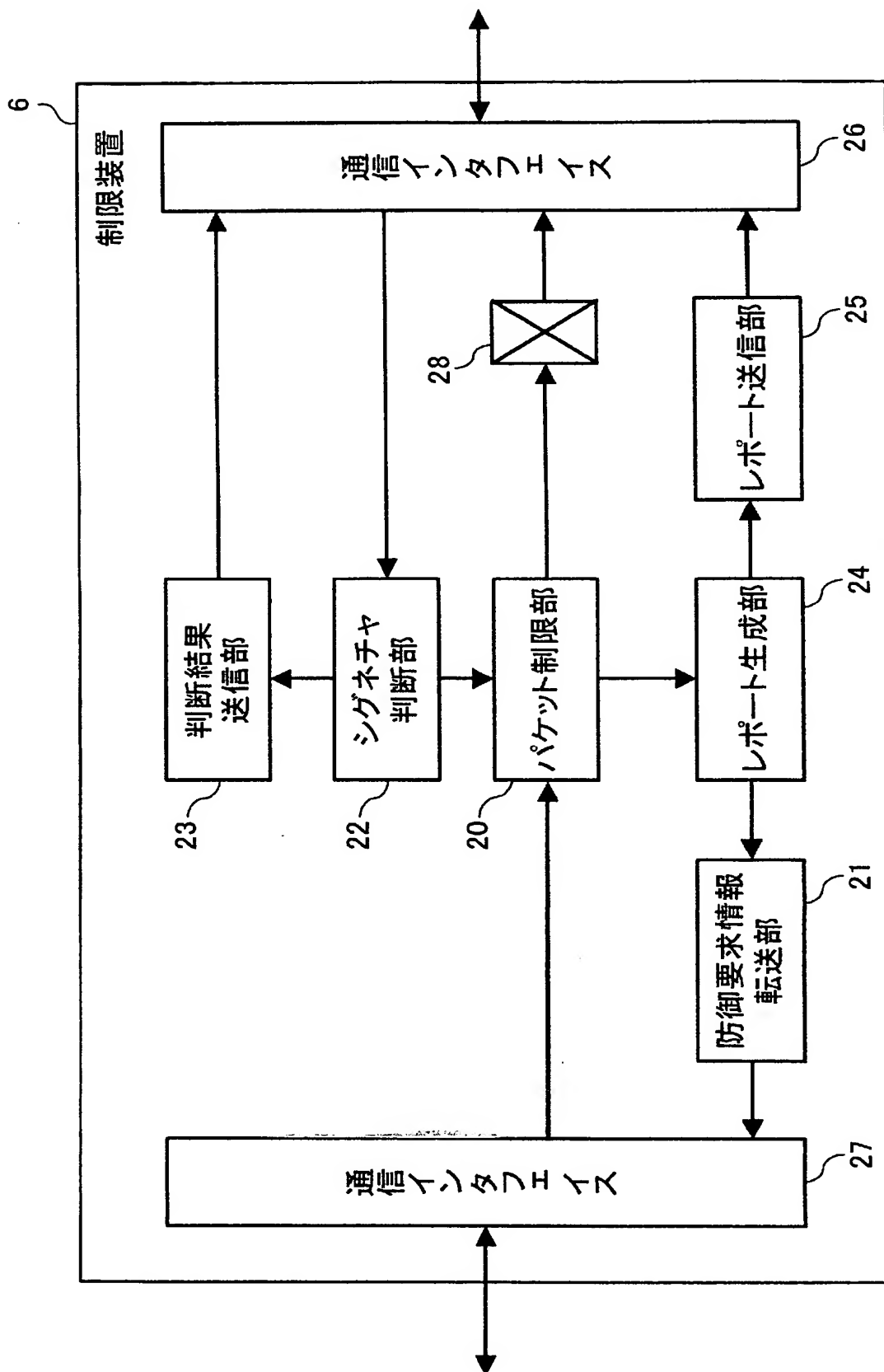
【0080】

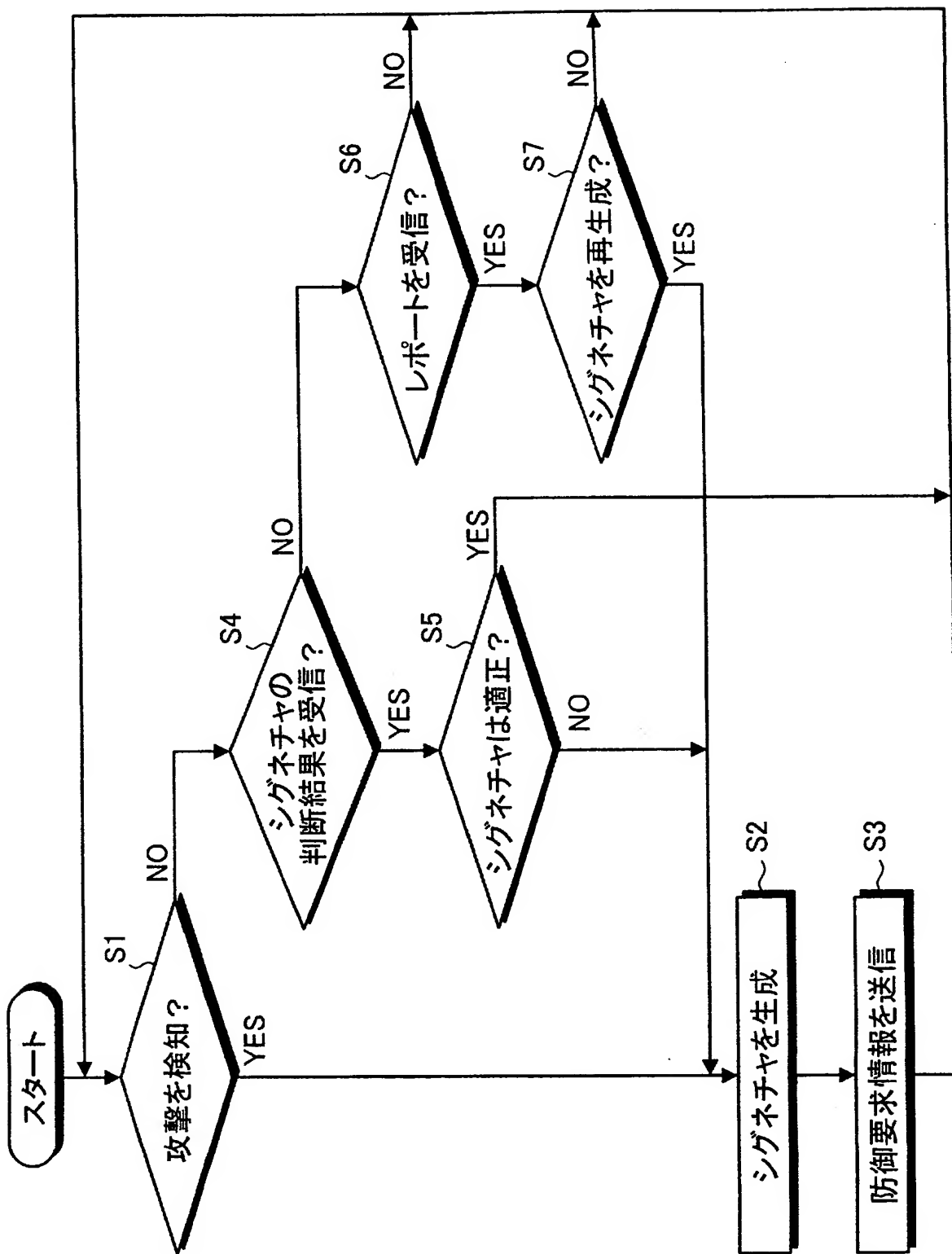
- 1 サービス不能攻撃防御システム
- 2 LAN
- 3 通信機器
- 4 ISP網
- 5 パケット監視装置
- 6、8、9 パケット制限装置
- 7 伝送路
- 10 攻撃検知部
- 11 防護要求情報送信部
- 12 シグネチャ生成部
- 13、14、26、27 通信インタフェース
- 15、28 スイッチ
- 20 パケット制限部
- 21 防護要求情報転送部
- 22 シグネチャ判断部
- 23 判断結果送信部
- 24 レポート生成部
- 25 レポート送信部

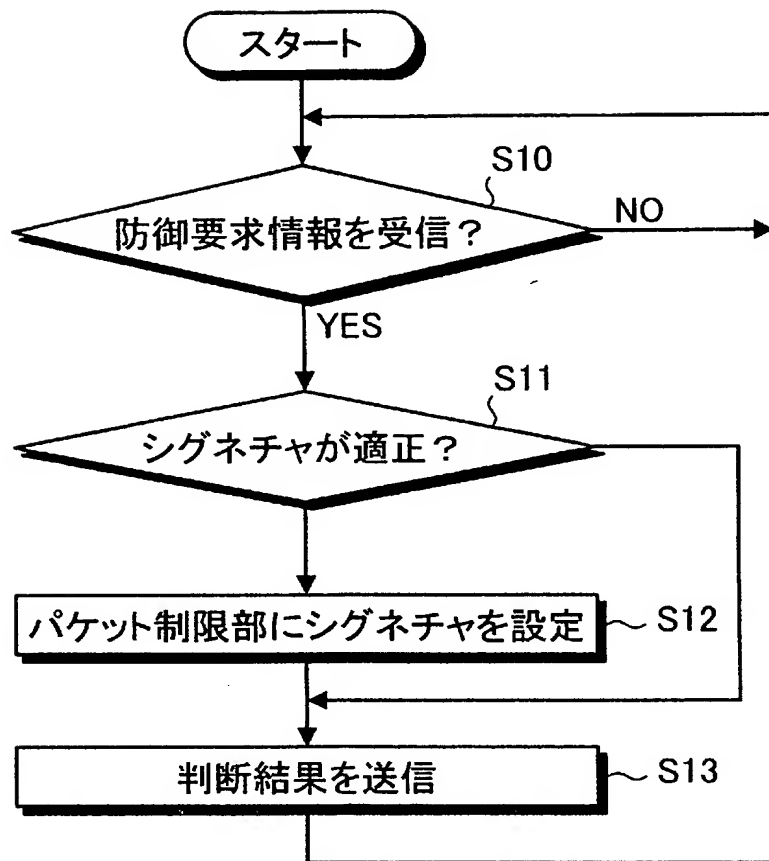


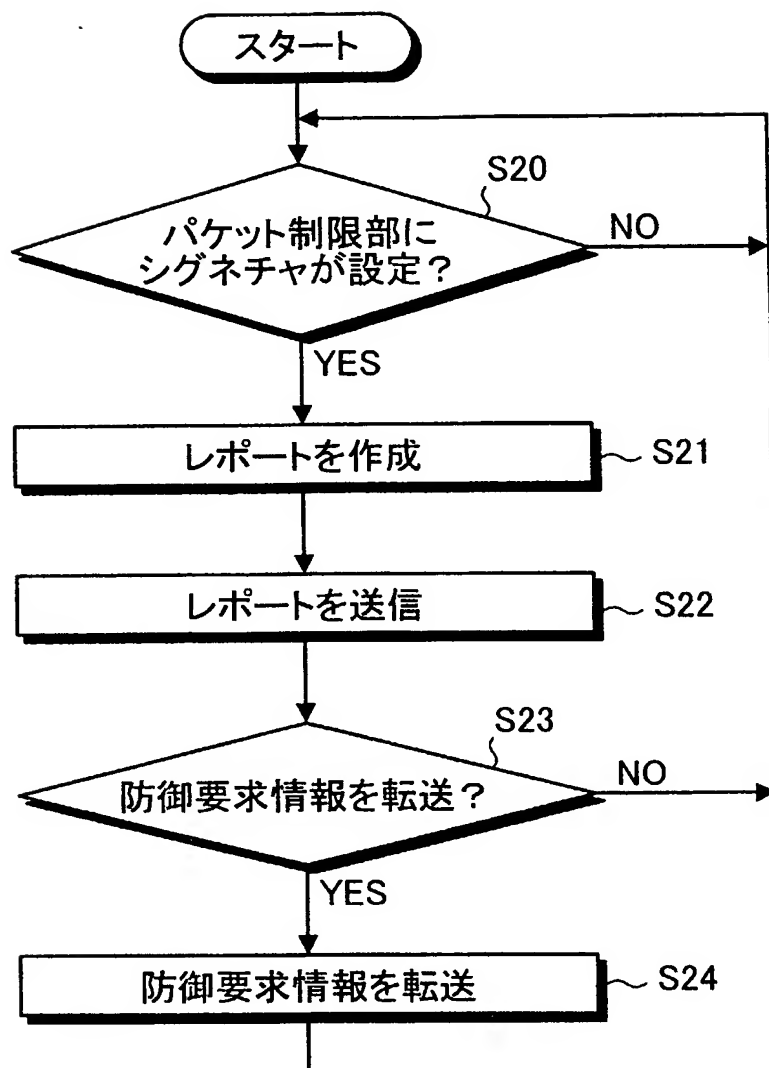


	検知属性	検知閾値	検出時間
1	[Dst=192.168.1.1/32, Protocol=TCP, Port=80]	500kbps	10秒
2	[Dst=192.168.1.2/32, Protocol=UDP]	300kbps	10秒
3	[Dst=192.168.1.0/24]	1Mbps	20秒









【要約】

【課題】ISPが通信の秘密を順守すると共に本来業務の範囲を逸脱しない形で、サービス不能攻撃から通信機器を防御することができるサービス不能攻撃防御システムを提供することを課題とする。

【解決手段】LAN2に設けられ、LAN2に接続された少なくとも1つの通信機器3にISP網4を介して送信されたパケットを監視する監視装置5と、ISP網4内に設けられ、LAN2に向かうパケットを制限する制限装置6とを備え、監視装置5は、通信機器3に対するパケットによる攻撃を検知し、検知した攻撃に対する防御の要求を表す防御要求情報を制限装置6に送信し、制限装置6は、防御要求情報に基づいてISP網4を介して通信機器3に送信されるパケットを制限する。

【選択図】

図1

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/015155

International filing date: 19 August 2005 (19.08.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-298244
Filing date: 12 October 2004 (12.10.2004)

Date of receipt at the International Bureau: 29 September 2005 (29.09.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse